Symantec

DATA SHEET

Symantec Endpoint Protection 15

The most complete and integrated endpoint security solution—cloud-delivered with AI-guided policy management

At a Glance

Enhanced security efficacy

- Unmatched efficacy via interlocking prevention technologies using artificial intelligence (AI) techniques (advanced machine learning and behavior analysis) coupled with time-tested prevention technologies
- Strengthened security posture with intelligence gathered by deception technology when attackers trigger easy-to-implement deceptors
- Unparalleled endpoint visibility and protection with telemetry from the world's largest civilian threat intelligence network

Simplified management

- Manage complete endpoint security from single cloud console
- Reduce update fatigue with minimal footprint of Symantec single agent stack
- Use AI-guided security management to drive more accurate policy updates, fewer misconfigurations, and greater administrative productivity to improve overall security hygiene

Broadest integrations

- Orchestrated defense and response at the endpoint quickly stop the attack's spread via integrations across Symantec portfolio
- Deeper visibility and reduced complexity using shared intelligence across Symantec Integrated Cyber Defense Platform and extensive integrations across Symantec and third-party products
- Strong security posture via open APIs to coordinate with third-party IT security solutions (e.g., orchestration, automation, ticketing, and SIEM)

Introduction

Attackers are using more sophisticated attacks to infiltrate networks, and the endpoint represents the last line of defense. Ransomware attacks are trending upward as evidenced by the WannaCry and Petya outbreaks. In addition, attackers' expanding use of fileless and stealthy attacks combined with 'living off the land' (using common IT tools for attacks) techniques threatens the confidentiality, integrity, and availability of endpoint assets.

So, what can security teams do to address cyber attacks? Managing multiple point products and technologies is overwhelming, and challenges mount when managing security across multiple geographies with diverse operation systems and platforms. With limited resources and limited budgets, security teams want easy-to-manage technologies that integrate with each other to improve overall security. They do not need just another point product. See Figure 1.

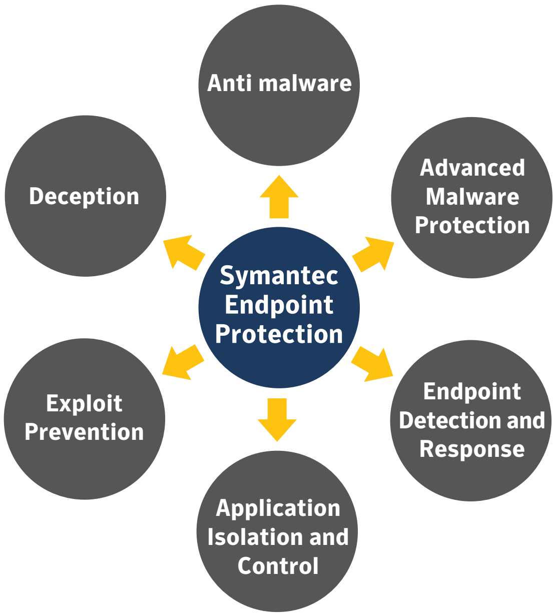

Anti malware
Deception
Advanced Malware Protection
Symantec Endpoint Protection
Exploit Prevention
Endpoint Detection and Response
Application Isolation and Control

Figure 1. Symantec offers complete endpoint security

Symantec Endpoint Protection (SEP) delivers superior, multilayer protection to stop threats regardless of how they attack your endpoints. SEP integrates with your existing security infrastructure to provide orchestrated responses that address threats quickly. The single, lightweight SEP agent offers high performance without compromising productivity, so that you can focus on your business. SEP enables security personnel to execute on many security use cases as outlined in Figure 2.

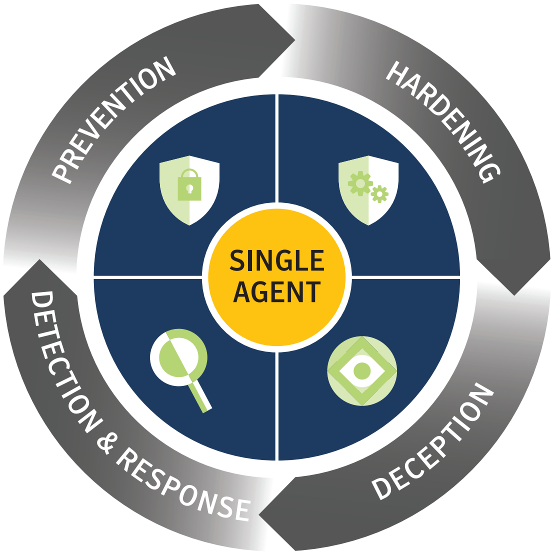


Figure 2. The SEP Security Framework

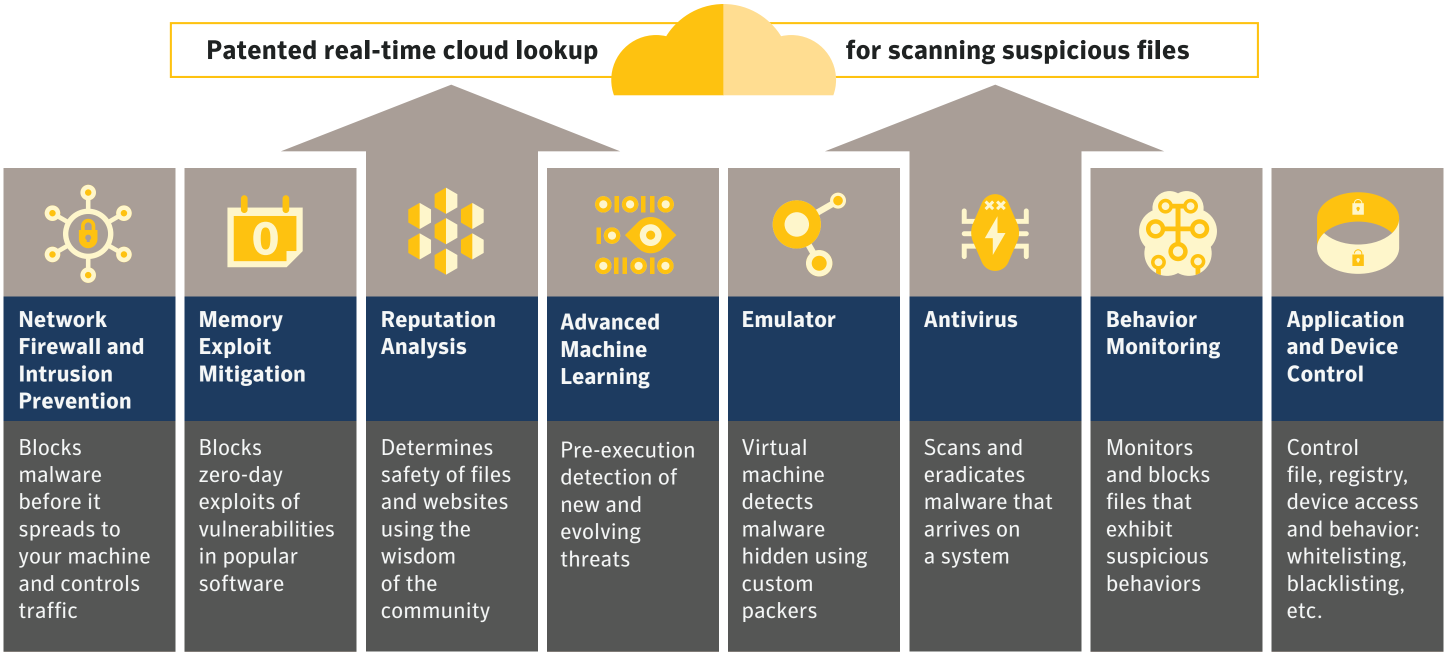
Enhanced security efficacy

Prevention

SEP protects endpoints regardless of where attackers strike on the attack chain as shown in Figure 3. SEP security efficacy leads the industry as validated by third parties. This level of prevention is only possible with a combination of proven, core technologies and new, innovative technologies.

Signatureless technologies

- **Advanced machine learning**—Detects new and evolving threats before they execute.
- **Memory exploit mitigation**—Blocks zero-day exploits of vulnerabilities in popular software.
- **Behavior monitoring**—Monitors and blocks files that exhibit suspicious behaviors.



Patented real-time cloud lookup **for scanning suspicious files**

Network Firewall and Intrusion Prevention
Blocks malware before it spreads to your machine and controls traffic

Memory Exploit Mitigation
Blocks zero-day exploits of vulnerabilities in popular software

Reputation Analysis
Determines safety of files and websites using the wisdom of the community

Advanced Machine Learning
Pre-execution detection of new and evolving threats

Emulator
Virtual machine detects malware hidden using custom packers

Antivirus
Scans and eradicates malware that arrives on a system

Behavior Monitoring
Monitors and blocks files that exhibit suspicious behaviors

Application and Device Control
Control file, registry, device access and behavior: whitelisting, blacklisting, etc.

Figure 3. SEP delivers multilayered prevention

Advanced capabilities

- **Global Intelligence Network (GIN)**—The world's largest civilian threat intelligence network collects data from millions of attack sensors; that data is analyzed by more than a thousand highly skilled threat researchers to provide unique visibility into threats.
- **Reputation Analysis**—Determines safety of files and websites using artificial intelligence techniques in the cloud and powered by the GIN.
- **Emulator**—Uses a lightweight sandbox to detect polymorphic malware hidden by custom packers.

- **Intelligent threat cloud**—Rapid scan capabilities using advanced techniques such as pipelining, trust propagation, and batched queries has made it unnecessary to download all signature definitions to the endpoint to maintain a high level of effectiveness. Only the newest threat information is downloaded, reducing the size of signature definition files by up to 70 percent, which in turn reduces bandwidth usage.
- **Roaming client visibility**—Receives critical events from clients that are off the corporate network.
- **Suspicious file detection**—Enables IT security teams to tune the level of detection and blocking separately to optimize protection and gain enhanced visibility into suspicious files for each customer environment.

Core capabilities

- **Antivirus**—Scans for and eradicates malware that arrives on a system.
- **Firewall and intrusion prevention**—Blocks malware before it spreads to the machine and controls traffic.
- **Application and device control**—Controls file, registry, and device access and behavior; also offers whitelisting and blacklisting.
- **Power Eraser**—An aggressive tool, which can be triggered remotely, to address advanced persistent threats and remedy tenacious malware.
- **Host integrity**—Ensures endpoints are protected and compliant by enforcing policies, detecting unauthorized changes, and conducting damage assessments; it can also isolate a managed system that does not meet your requirements.
- **System lockdown**—Allows whitelisted applications (known to be good) to run or blocks blacklisted applications (known to be bad) from running.

In all, the single-agent architecture enables IT security teams to add innovative security technology without having to add new agents. In addition, SEP supports many environments, now including IPv6.

Mobile capabilities

For roaming users, Symantec offers add-on defenses that deliver dynamic protection that complements endpoint security to address attack vectors for modern devices and user behavior for Windows 10.

Cloud connect defense

- **Network integrity protection**—Identifies rogue Wi-Fi networks and utilizes hotspot reputation technology.
- **Smart VPN**—Delivers policy-driven VPN to protect network connections and support compliance.
- **Easy management**—Uses the same cloud console for all endpoint security.
- **Flexible deployment**—Offers universal Windows app downloadable from the Microsoft App Store and mobile device management (MDM)-based deployment options.
- **ARM-processor support**—Offers standalone protection for Windows 10 in S mode for devices with Snapdragon processors as well as Intel and AMD.

Hardening

Hardening consists of several add-on capabilities that complement SEP prevention to deliver unprecedented efficacy against malware and suspicious applications. It includes advanced application defenses that deliver fast time to value by using the same SEP agent. It minimizes the attack surface by controlling which applications can run and what these applications can do.

The advanced application protection solutions share some capabilities. They offer comprehensive application discovery to find all apps on the endpoint and conduct a risk assessment on the apps and their respective vulnerabilities. These solutions also promote high employee productivity by fully supporting standard employee workflows.

Application isolation

- Hardens endpoints by isolating suspicious or malicious apps into ‘jail mode’ to prevent the execution of privileged operations including downloading executable files, writing to the registry, and more.
- Strengthens protections by shielding productivity tools and other known good applications from vulnerability exploits.
- Maximizes security efficacy by complementing critical hardening technology with SEP prevention capabilities.

Application control

- Delivers fixed-function device lock-down by enforcing default-deny to applications and restricting updates to those defined as trusted.
- Offers restricted execution of unauthorized apps for standard endpoints by governing the ‘allow’ list of approved apps for additional flexibility.
- Easily extends the use of unapproved applications when deemed safe while alerting administrators of potential risks posed by application drift.
- Maximizes security efficacy by complementing critical hardening technology with SEP prevention capabilities.

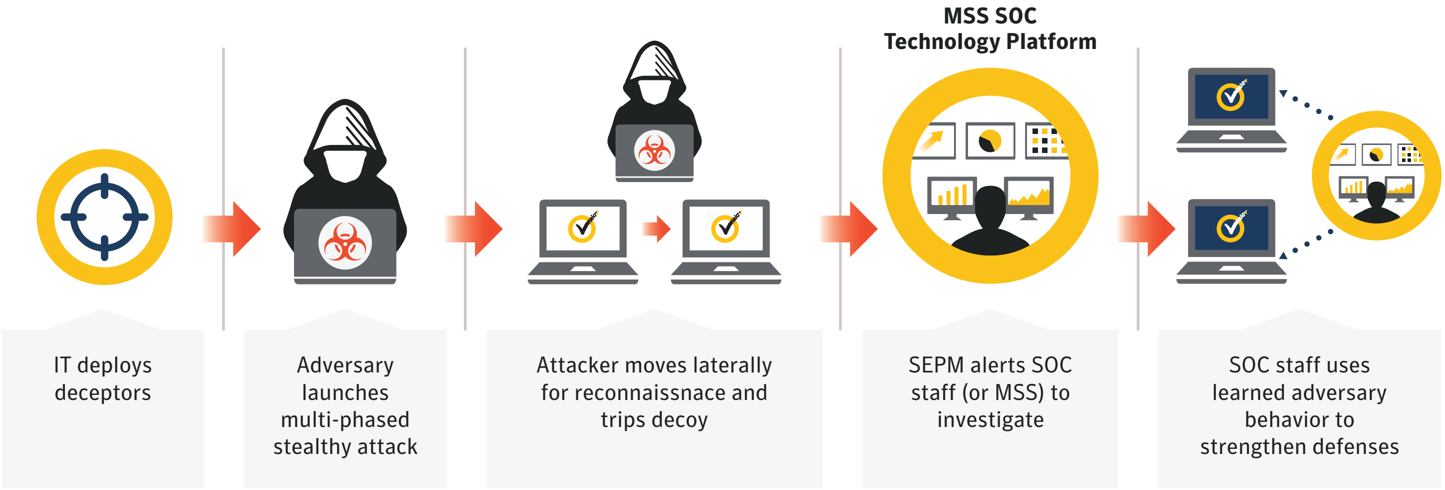

MSS SOC Technology Platform
IT deploys deceptors
Adversary launches multi-phased stealthy attack
Attacker moves laterally for reconnaissnace and trips decoy
SEPM alerts SOC staff (or MSS) to investigate
SOC staff uses learned adversary behavior to strengthen defenses

Figure 4. How Deception works

Symantec also offers comprehensive defense for corporate domains by combining AI, obfuscation, and advanced forensics methodologies to quickly detect and automatically contain advanced persistent threats at the point of breach.

Threat Defense for Active Directory

- Disrupts domain reconnaissance, lateral movement, and credential theft activities employed by attackers by using Active Directory (AD) obfuscation and policy-driven process, device, and user analysis.
- Uses automated attack simulations to expose domain and AD service vulnerabilities and provides recommendations on remediation.
- Delivers full forensic reporting within a few seconds of true threat alerts to provide a snapshot of the machine at the time of attack along with full attack chain analysis.
- Utilizes auto mitigation to contain an attacking process of the source host, thus removing its ability to spawn another process, run recon commands, or communicate out to the network.

Deception

SEP includes the capability to plant deceptors (i.e., bait) for exposing hidden adversaries and revealing attacker intent and tactics via early visibility, so that the information can be used to enhance your security posture. It features accurate and insightful detection while delivering fast time to value. Joint SEP and Symantec Managed Security Services customers benefit from 24x7 real-time deception monitoring and response by a global team of experts. Symantec is the only endpoint protection platform vendor offering deception.

SEP:

- Uses lures and baits for active security to expose and delay attackers.
- Determines attacker intent to improve security posture.
- Delivers deception at scale to simplify rollout and management.

Endpoint Detection and Response (EDR)

Symantec Endpoint Detection and Response provides incident investigation and remediation using the integrated EDR capabilities in SEP. Cloud-based artificial intelligence, precision machine learning, behavioral analytics, and threat intelligence minimize false positives and ensure high levels of productivity for security teams. The security team can roll out the solution within an hour to expose advanced attacks. Symantec Endpoint Detection and Response capabilities allow incident responders to quickly search, identify, and contain all impacted endpoints while investigating threats using on-premises and cloud-based sandboxing. In addition, continuous recording of system activity supports full endpoint visibility and real-time queries.

EDR and Targeted Attack Analytics

The integration of Targeted Attack Analytics (TAA) with Endpoint Detection and Response solves critical security challenges. TAA combines local and global telemetry, artificial intelligence, and attack research to expose attacks that would otherwise evade detection.

Using TAA, Endpoint Detection and Response (ATP: Endpoint) customers benefit from ongoing delivery of new attack analytics and generation of custom incidents, covering detailed analysis of attacker methods, impacted machines, and remediation guidance—all at no additional cost.

Symantec Endpoint Detection and Response:

- **Detects and exposes**—Reduces time to breach discovery and quickly exposes scope.
- **Investigates and contains**—Increases incident responder productivity and ensures threat containment.
- **Resolves**—Rapidly fixes endpoints and ensures threat does not return.
- **Enhances Security Investments**—Takes advantage of prebuilt integrations and public APIs.

Simplified management

Symantec Cyber Defense Manager, Symantec's cloud-based management console for endpoint security, drives more accurate, intelligent, and faster insights with AI-guided security management from a single console.

Cyber Defense Manager:

- **Full cloud console**—Manages complete endpoint security from a single cloud console to reduce endpoint security management complexity.
- **Single SEP agent**—Reduces update fatigue with minimal footprint of Symantec single agent stack.
- **AI-guided security management**—Drives more accurate policy updates, fewer misconfigurations, and greater administrator productivity to help improve overall security hygiene.
- **Autonomous security management**—Learns from administrators or the organization or community to continuously assess and strengthen security posture.
- **Simplified workflows**—Uses simplified workflows with context-aware recommendations to eliminate routine tasks and enhance endpoint security decisions.

For organizations that require on-premises or hybrid management options, SEP can accommodate that too.

Broadest integrations

Most large organizations support global IT environments that are becoming increasingly complex. Many solutions, however, only do a very specific job. Therefore, organizations need an endpoint protection solution that provides greater value and better overall protection by integrating with other IT security solutions to share intelligence and defend the network together.

SEP 15 is a foundational product that facilitates integration so that IT security teams can detect threats anywhere in their network and address these threats with an orchestrated response. SEP 15 works alongside Symantec solutions (as a key component of the Integrated Cyber Defense Platform) and with third-party products (via published APIs) to strengthen your security posture. The Symantec Integrated Cyber Defense Platform unifies cloud and on-premises security to protect users, information, messaging and the web, powered by unparalleled threat intelligence. No other vendor provides an integrated solution that orchestrates a response at the endpoint (blacklists and remediation) triggered by the detection of a threat at the network gateway (i.e., web and email security gateways).

Advanced Symantec integrations

- **Content analysis integration**—Utilizes dynamic sandboxing and additional engines for further analysis of suspicious files.
- **Multifactor authentication integration**—Supports Symantec Validation and ID Protection and PIV/CAC smart cards for authentication into the SEP Manager console.
- **Web Security Service integration**—Redirects web traffic from roaming users to Symantec Web Security Service using a PAC file.
- **Secure Web Gateway integration**—Programmable REST APIs make integration possible with existing security infrastructure including Symantec Secure Web Gateway, orchestrating a response at the endpoint to quickly stop the spread of infection.

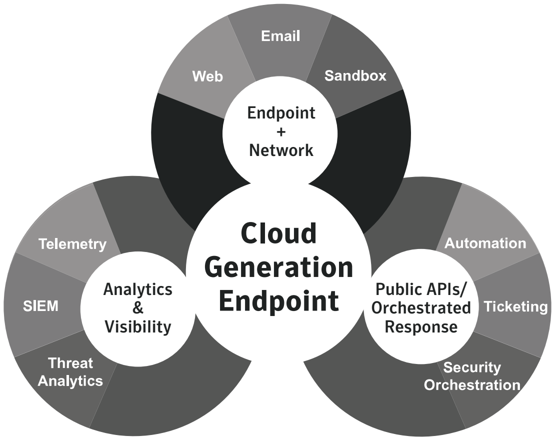


Figure 5.

High-performance, lightweight solution to enable productivity

Large or frequent content updates take up bandwidth, reduce endpoint performance, and compromise productivity. Optimizing content updates and delivering better detection of threats is a win-win. These capabilities reduce the IT team's burden for scheduling frequent security updates. And users do not have the hassle of security updates impacting productivity.

SEP has a strong record for delivering better protection with better performance and lower bandwidth requirements. Symantec consistently scores at the top in third-party performance tests including Passmark Software's Enterprise Endpoint Security Performance Benchmark tests for Windows 7 and Windows 10. Visit the Symantec Performance Center for additional third-party validation: **symantec.com/products/performance-center**.

Compared to products from emerging vendors, SEP offers less endpoint complexity by bundling multiple capabilities in a single, lightweight agent. Attempting to match Symantec endpoint security capabilities would require multiple vendors, multiple solutions, and certainly multiple agents.

System requirements

Client Workstation and Server System Requirements*

Windows® Operating Systems

- Windows 7 (32-bit, 64-bit; RTM and SP1)
- Windows Embedded 7 Standard, POSReady, and Enterprise (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows Embedded 8 Standard (32-bit and 64-bit)
- Windows 8.1 (32-bit, 64-bit), including Windows To Go
- Windows 8.1 update for April 2014 (32-bit, 64-bit)
- Windows 8.1 update for August 2014 (32-bit, 64-bit)
- Windows Embedded 8.1 Pro, Industry Pro, and Industry Enterprise (32-bit, 64-bit)
- Windows 10 (32-bit, 64-bit)
- Windows 10 November Update (version 1511) (32-bit, 64-bit)
- Windows 10 Anniversary Update (version 1607) (32-bit, 64-bit)
- Windows 10 Creators Update (version 1703) (32-bit, 64-bit)
- Windows 10 Fall Creators Update (version 1709) (32-bit, 64-bit)
- Windows 10 April 2018 Update (version 1803) (32-bit, 64-bit)
- Windows 10 October 2018 Update (version 1809) (32-bit, 64-bit)
- Windows Server 2008 R2 (32-bit, 64-bit; R2, SP1, and SP2)
- Windows Small Business Server 2008 (64-bit)
- Windows Essential Business Server 2008 (64-bit)
- Windows Small Business Server 2011 (64-bit)
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Windows Hardware Requirements

- 32-bit processor: 2 GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended)
- 64-bit processor: 2 GHz Pentium 4 with x86-64 support or equivalent minimum
- 1 GB of RAM (2 GB recommended)
- 530 MB of free space on the hard disk

Macintosh® Operating Systems

- Mac OS X 10.10, 10.11, macOS 10.12, 10.13, 10.14

Mac Hardware Requirements

- 64-bit Intel Core 2 Duo or later
- 2 GB of RAM
- 500 MB of free space on the hard disk

Virtual Environments

- Microsoft Azure
- Amazon WorkSpaces
- VMware WS 5.0, GSX 3.2 or later, ESX 2.5 or later
- VMware ESXi 4.1 – 5.5
- VMware ESX 6.0
- Microsoft Virtual Server 2005
- Microsoft Windows Server 2008, 2012, and 2012 R2 Hyper-V
- Citrix XenServer 5.6 or later
- Virtual Box by Oracle

Management Console System Requirements

Windows® Operating Systems

- Windows Server 2008 (64 bit)
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Web Browser

- Microsoft Internet Explorer 11
- Mozilla Firefox 5.x through 60
- Google Chrome 66
- Microsoft Edge

Symantec Endpoint Protection client must run one of the following Windows desktop operating systems to run Symantec Endpoint Protection Hardening:

- Windows 7 (RTM and SP1), Professional, Enterprise
- Windows 8, Professional, Enterprise
- Windows 8.1 (update for April 2014 and August 2014; Windows To Go), Professional, Enterprise
- Windows 10 (RTM), Professional, Enterprise
- Windows 10 November Update (version 1511), Professional, Enterprise
- Windows 10 Anniversary Update (version 1607), Professional, Enterprise
- Windows 10 Creators Update (version 1703), Professional, Enterprise
- Windows 10 Fall Creators Update (version 1709), Professional, Enterprise
- Windows 10 April 2018 Update (version 1803), Professional, Enterprise
- Windows 10 October 2018 Update (version 1809), Professional, Enterprise (32-bit, 64-bit)

* System requirements are for SEP 15. For a complete list of system requirements visit our support page.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments, and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud, and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com